UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/084,436 | 02/28/2002 | Zhichen Xu | 10018744-1 | 6233 |

7590 10/19/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER | |
|---|---|
| LEMMA, SAMSON B | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/084,436 | XU ET AL. | |
| | Examiner | Art Unit | |
| | Samson B. Lemma | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *28 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## *DETAILED ACTION*

1. Claims **1-36** have been examined.

## *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1-2,8-19,24-25,31-36** are rejected under 35 U.S.C. 102(b) as being anticipated by Walker et al. (hereinafter referred as Walker) (U.S. Patent No 5,862,223)

4. **As per claim 1, 8,12,15,17-18, 24, 31-32 Walker discloses** a method of increasing peer privacy, comprising:[column 35, lines 14-17]

**Receiving a request for data from a data requester,**[column 35, 45-47; column 35, lines 15-17] (Bob's computer receives Alice request through the 3rd trusted party central controller/carol's computer as described on column 35, lines 33-34) **wherein said data is stored at a data provider;**[figure 2, ref. Num "270"] **selecting a plurality of peers to form a path,**[column 35, lines 14-17;column 36, lines 40-42] **wherein said data**

**provider and said data requester are the respective ends of said path**;[column 36, lines 40-42, column 35, lines 45-column 36, lines 42] **generating a mix according to said path; and transmitting said mix to said data provider** [column 36, lines 9-10 and figure 29].

5. **As per claim 2,16,19 and 25 Walker discloses** a method as applied to claim above. Furthermore Walker disclose the method further comprising: generating a first encryption key; and encrypting said first encryption key with a public encryption key of said data provider. **[[column 35, lines 63-column 36, line 6](**The first encryption key is a key k_3 is generated by carol/the 3rd trusted peer/computer and the first encryption key generated by carol which is K_3 is also protected or encrypted with the public key of Bob as shown on column 36, lines 3, x_3, and line 11)

6. **As per claim 9-11,13-14, 33-36 Walker discloses a method of increasing peer privacy, comprising: receiving a message comprising a mix at a current peer**[column 35, lines 63, carol receives message comprising mix from Alice]; **modifying said mix by applying a complementary encryption key of said current to said mix**;[column 36, lines 7, M_1 which modifies said mix by applying encryption key] **retrieving a subsequent peer to said current peer; modifying said message with said modified mix; and transmitting said modified message to said subsequent peer.[column 36, lines 11, c, carlos after retrieving a subsequent peer/bob to said current peer/carol; it modifies said message with said modified mix and send it to subsequent peer bob as it is described on column 35, lines 63-column 36, lines 11 and figure 29]**

## *Claim Rejections - 35 USC § 103*

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 3-7,20-23,26-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (hereinafter referred as Walker) (U.S. Patent No 5,862,223) in view of Herz (hereinafter referred as Herz) ((U.S. Patent No 6,460,036) (filed on Dec 5, 1997)

9. **As per claim 22 Walker discloses** an apparatus for increasing privacy in a data requester, comprising: at least one processor; memory coupled to said at least one processor; and a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider, said message comprises:

> A mix configured to provide a path among a plurality of peers [Column 35,lines 14-18]; **an encrypted reference to requested data encrypted with a first encryption key [column 35, lines 63-column 36, line 6]**(the first encryption key is a key generated by carol/the 3rd trusted peer/computer and the reference

which is included in the message from Alice is encrypted as shown on column 36, lines 6**]; an encrypted first encryption key protected with a public key of said data requester;** [Column 35, lines 36-column 36, line 10] (encrypted first encryption key generated by carol which is K_3 is also protected or encrypted with the public key of Bob) **and said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider [column 36, lines 11-13] (Bob receives M_1 and decrypt the first encryption key K_3 with a complementary/private key of BOB)**

**Walker** does not explicitly disclose decrypting data reference with said encryption key

- However, in the field of endeavor **Herz** discloses,

The user's client processor C3 forms a signed message **S(R, SK.sub.P),** which is paired with the user's pseudonym P and (if the request R requires airesponse) a secure one-time set of return envelopes, to form a message M. It protects the message M with a multiply enveloped route for the outgoing path. The enveloped route s provide for secure communication **between S1 and the proxy server S2**. The message M is enveloped in the most deeply nested message and is therefore difficult to recover should the message be intercepted by an eavesdropper. 2. The message M is sent by client C3 to its local server S1, and is then routed by the data communication network. **N from server S1 through a set of mixes as dictated by the outgoing envelope set and arrives** at the **selected proxy server S2.** 3. The proxy server **S2 separates the received message M into the request message R, the pseudonym P, and (if included) the set of envelopes for the return path. The proxy server S2 uses pseudonym P to index and retrieve the corresponding record in proxy server S2's database**, which record

is stored in local storage at the proxy server S2 or on other distributed storage media accessible to. proxy server S2 via the network N. This, record contains a public key PK.sub.P, user-specific information, and credentials associated with pseudonym P. The proxy server S2 uses the public key PK.sub.P to check that the signed version S(R, SK.sub.P) of request message R is valid. [column 39, lines 8-35]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of adding data reference that is cryptographically protected and passed to the destination so that it will be used to retrieve the required data at the destination node as per teachings of **Hertz** into the method taught by **Walker**, in order to securely transfer data reference to destination node/provider node and securely retrieve the required data.

## *Conclusion*

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

09/28/2005

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100